Page 1, the last paragraph bridging pages 1 and 2:

Figure 1 is a diagram illustrating a conventional repeater network. The network 10 includes a repeater 12 configured for transmitting a data packet received on an input port to the other ports for reception by the respective network nodes 14. For example, assume that node (i.e., workstation) 14a transmits a data packet via the network medium 16. The transmitted data packet is received by a physical layer transceiver (PHY) 20a which recovers the digital data from the transmitted analog signal. As recognized in the art, the PHY transceiver 20a may be a 100 Base-TX IEEE standard 802.3u receiver, configured for receiving a 3-level MLT-3 encoded analog signal at a 125 Megabit per second rate, and configured for output of the transmit data as nibble-wide (4 bits) or byte-wide transmit data (TXD) to the MII 18 between the PHY 18 and the repeater 12. The repeater 12, upon receiving the transmit data from the PHY transceiver 20a, retransmits the transmit data to all the other ports for transmission by the other PHY transceivers (e.g., 20b, 20c, and 20d). The network stations 14 of the other ports will ignore the packet unless the destination address of the packet matches the network stations own address. One problem with the arrangement is that any network node can eavesdrop on all packets that are transmitted on the network. Hence, an unauthorized workstation 14e may eavesdrop on all data packets by obtaining access to a repeater port.

Page 7, the last paragraph bridging pages 7 and 8:

As shown in Figure 4, the state machine and the detection circuit 50 begins in the idle state 60, where the physical layer transceiver 36 receives idle symbols from the corresponding MII 40 and with both the transmit enable and transmit error signals equal to 0. Upon initial transmission of the data packet by the repeater core 32, the security circuitry 46 asserts the transmits enable (TX_EN) signal (TX_EN=1) until the entire destination address can be encoded. As shown in Figure 4, the transmit enable is asserted upon detection of a preamble (e.g., following detection of J and K symbols in sequence). The transmit enable signal is asserted on all repeater ports 34 until the destination address (DA) of the data packet 58 can be decoded. In response to detecting assertion of the transmit enable signal (TX_EN=1) and deassertion of the transmit error signal (TX_ER=0), the detection circuit 50 moves from state 60 to state 62 during the next clock cycle. If during state 62 the transmit enable signal is deasserted (TX_EN=0) or transmit error is asserted (TX_ER=1), the detection circuit returns to state 60. However, if the transmit enable signal is asserted concurrent with deassertion of the transmit error signal for another clock cycle, the detection circuit 50 moves to state 64. The detection circuit 50 remains in state 64 until deassertion of both the transmit enable and transmit errors signals (e.g., end of transmission), a detected error condition by concurrent assertion of both the transmit enable and transmit errors signals, or upon detection of a corruption state. The detection circuit 50 detects at state 64 the occurrence of a corruption by the concurrent assertion of the transmit error signal and deassertion of the transmit enable signal, causing the detection circuit 52 to move to the jam 1 state 66.